UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,904	06/28/2001	Yves Louis Gabriel Audebert	L741.01105	1582

7590 05/26/2005

STEVENS, DAVIS, MILLER & MOSHER, LLP
Suite 850
1615 L Street, N.W.
Washington, DC 20036

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/892,904	AUDEBERT ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/11/2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16 and 18-37* is/are pending in the application.

4a) Of the above claim(s) *17* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16 and 18-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

FINAL REJECTION

Response to Arguments

1. Applicant's arguments/amendments with respect to amended claims 1-3, 9, 13-16, 18-20, 22, and 26-28, original claims 4-8, 10-12, 21, 23-25, and 29, canceled claim 17, and added claims 30-37 have been considered but are moot in view of the new ground(s) of rejection.

2. Examiner accepts the amended abstract.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 13-16 and 18-37 are rejected under 35 U.S.C. 102(b) as being anticipated by Sudia et al. (Sudia, Patent No.: US 6,209,091 B1).

As per claim 13, Sudia teaches a data processing system for validating a key protection certificate generated by a PSD comprising:

data processing means (fig. 3 No. 44), data storage means (fig. 3 No. 52), communications means (fig. 3 No. 42), cryptography means (fig. 3 No. 46), a first securely shared secret key, a second securely shared secret key and a public key (col. 12 lines 18-col. 13 lines 50),

wherein the said cryptography means includes a message authentication code algorithm (col. 2 lines 16-44, col. 2 lines 52-67, col. 17 lines 39-42, and col. 18 lines 65-67), cross referencing means (col. 2 lines 52-55) and a comparator algorithm (col. 10 lines 13-14), and

wherein said cross referencing means comprises means for selecting proper first and second securely shared secret keys, a proper public key, proper cryptography algorithms (col. 10 lines 13-14, and col. 12 lines 18-col. 13 lines 50) and reference parameters associated with said key protection certificate (fig. 2 No. 38), by use of a unique device name of said PSD contained in said key protection certificate (col. 9 lines 37-57and col. 12 lines 47-49).

As per claims 26 and 34, Sudia teaches a method/apparatus for generating a key protection certificate comprising:

injecting a first securely shared secret key, a second securely shared secret key, a key protection algorithm and cryptographic seed information into a PSD which comprises a unique device name (col. 9 lines 36-56), wherein at least a portion of said seed information is used in generating at least one public key and one private key (col. 12 lines 18-col. 13 lines 50),

storing said injected first and second securely shared secret keys and said cryptographic seed information in a secure domain within said PSD (col. 6 lines 45-65, and col. 29 lines 24-37),

sending a command to said PSD for generating said at least one public key and one private key, wherein said command initiates generation of said keys and of said key protection certificate (col. 13 lines 66-col. 14 lines 13, col. 7 lines 58-62, col. 19 lines 19-21, and col. 15 lines 13-30),

generating said at least one public key and said one private key using at least a portion of said seed information (col. 12 lines 18-col. 13 lines 50, col. 15 lines 13-30),

generating contextual attributes specific to at least the generation of said private key (col. 23 lines 27-50),

encrypting at least a portion of said contextual attributes using said first securely shared secret key, forming private contextual attributes and public contextual attributes, wherein predetermined parameters are included in said private contextual attributes (col. 23 lines 27-59),

storing said public key and said private key in said secure domain within said PSD (col. 6 lines 45-65, col. 29 lines 24-37),

generating a digital signature of s said unique device name using said private key (col. 8 lines 33-46),

concatenating said unique device name, said private contextual attributes, said public contextual attributes with said digital signature and generating a first intermediate result (fig. 6 No. 107, col. 26 lines 12-13; Header including a clear unique device name is combined with private and public contextual attributes, and digital signature to form a first intermediate result),

generating a message authentication code of said first intermediate result using said second securely shared secret key producing a second intermediate result (col. 14 lines 16-44; hash is generated to form a second intermediate result),

concatenating said first intermediate result with said second intermediate result producing said key protection certificate (col. 14 lines 16-57; hash is combined with the header including a clear unique device name, private and public contextual attributes, digital signature to form a first intermediate result); and

storing said key protection certificate in said secure domain within said PSD (col. 15 lines 59-64).

As per claims 27 and 36, Sudia teaches a method/apparatus for validating a key protection certificate generated by a PSD comprising:

receiving said key protection certificate, wherein said certificate contains at least a plain text device name portion (col. 26 lines 1-13; header having device name in clear), a signed device name portion (col. 7 lines 29-30, and col. 14 lines 1-41; certificate is signed and the signed certificate includes device name) and cryptogram portion (col. 14 lines 23-25),

cross-referencing said device name with proper first and second securely shared secret keys, proper public key, proper cryptographic algorithms and reference parameters associated with said key protection certificate (col. 16 lines 32-65, and col. 15 lines 13-64),

verifying said signed device name portion of said certificate using said proper public key (col. 6 lines 54-65),

comparing the resulting device name with said device name portion included in said certificate (col. 14 lines 1-4, 51-53, and col. 8 lines 33-46),

independently performing a message authentication code function on said concatenated private contextual attributes, public contextual attributes, device name, and signed device name portions of said certificate using a first of said proper securely shared secret keys (col. 14 lines 1-44),

comparing the resulting message authentication code with a method authentication code included in said certificate (col. 10 lines 10-22),

decrypting said private contextual attributes using a second of said proper securely shared secret keys (col. 23 lines 51-59, and col. 22 lines 63-68),

comparing at least a portion of the private contextual attributes to the reference parameters (col. 23 lines 46-50, and col. 18 lines 65-66),

validating said certificate if said resulting device name (col. 26 lines 1-13) matches said device name contained in said certificate (col. 14 lines 1-4, 51-53, and col. 8 lines 33-46), said independently generated message authentication code matches said message authentication code contained in said certificate (col. 10 lines 10-25) and at least a portion of said private contextual attributes matches said reference parameters (col. 23 lines 51-59, and col. 22 lines 63-68),

rejecting said certificate if any of said matches is not achieved (col. 10 lines 10-17).

As per claim 30, Sudia teaches a data processing system for generating a key protection certificate comprising a PSD (Fig. 3 No. 55) further comprising a unique device name (col. 6 lines 28-30, 45-47, 57-61, col. 9 lines 17-21), at least one cryptographic key generating algorithm (col. 10 lines 63-64), a key protection certificate generating algorithm (col. 9 lines 37-57and col. 12 lines 47-49), data processing means (fig. 3 No. 44), data storage means (fig. 3 No. 52) and communications means (fig. 3 No. 42), wherein said key protection certificate generating algorithm comprises means for producing sequentially with said cryptographic key generating algorithm (col. 2 lines 49-67, and fig. 24), upon completion of cryptographic key generation, a unique digital certificate that comprises said unique device name and depends on said generated cryptographic key (col. 8 lines 36-58, and col. 14 lines 1-4).

As per claim 31, Sudia teaches a data processing system for validating a key protection certificate generated by a PSD (Fig. 3 No. 55) comprising data processing means (fig. 3 No. 44), data storage means (fig. 3 No. 52), communications means (fig. 3 No. 42), cryptography means (col. 10 lines 63-64), at least one cryptographic key (col. 10 lines 63-64), and cross referencing means, wherein cross referencing means comprises means for selecting at least one proper cryptographic key and one proper cryptography algorithm associated with said key protection certificate (col. 10 lines 13-14, and col. 12 lines 18-col. 13 lines 50), by use of a unique device name of said PSD contained in said key protection certificate (col. 9 lines 37-57and col. 12 lines 47-49).

As per claims 32 and 35, Sudia teaches a method/apparatus for generating a key protection certificate comprising sending a command to a PSD comprising a unique device name for generating at least one cryptographic key (col. 7 lines 58-62, col. 19 lines 19-21, and col. 15 lines 13-30), wherein said command initiates generation by said PSD of said key and of said key protection certificate that comprises said unique device name of said PSD and depends on said generated cryptographic key (col. 13 lines 66-col. 14 lines 13).

As per claims 33 and 37, Sudia teaches a method/apparatus for validating a key protection certificate generated by a PSD comprising:

receiving said key protection certificate, wherein said certificate contains at least a unique device name of said PSD (col. 14 lines 1-4),

cross-referencing said device name with at least one proper cryptographic key and one proper cryptography algorithm associated with said key protection certificate (col. 16 lines 32-65, and col. 15 lines 13-64), and

validating said key protection certificate with at least said proper cryptographic key and said proper cryptography algorithm (col. 12 lines 50-53).

As per claim 14, Sudia discloses the system, wherein said proper first securely shared secret key, said proper second securely shared secret key and said public key have a direct generation relationship with said key protection certificate (col. 12 lines 13-col. 13 lines 50).

As per claim 15, Sudia discloses the system, wherein said communications means includes means for transmitting requests for said key protection certificate and means for receiving said key protection certificate (fig. 1 No. 21).

As per claim 16, Sudia discloses the system, wherein said received key protection certificate includes private contextual attributes, public contextual attributes, said unique a device name of said PSD, a signed device name and a message authentication code in dependence on said private contextual attributes, said public contextual attributes, said unique device name of the PSD, and said sinned device name (fig. 6 No. 107, col. 26 lines 12-13, and col. 14 lines 41-45; Header including a clear unique device name is combined with private and public contextual attributes, digital signature, and hash).

As per claim 18, Sudia discloses the system, wherein said signed device name is decrypted using said proper public key, generating a second device name (col. 2 lines 52-55).

As per claim 19, Sudia discloses the system, wherein said second device name and said unique device name of said PSD contained in said certificate are compared by the, comparator algorithm to determine if said second device name and said unique device name of said PSD contained in said certificate match (col. 26 lines 1-13, col. 14 lines 1-4, 51-53, and col. 8 lines 33-46).

As per claim 20, Sudia discloses the system, wherein a second message authentication code is generated using said private contextual attributes, said public contextual attributes, said unique device name of said PSD, said signed device name included in said certificate and said proper second securely shared secret key as inputs into said message authentication code algorithm (col. 14 lines 16-44).

As per claim 21, Sudia discloses the system, wherein said second message authentication code and said message authentication code contained in said certificate are compared using said comparator algorithm to determine if said second message authentication code and said message authentication code contained in said certificate match (col. 10 lines 10-22).

As per claim 22, Sudia discloses the system, wherein said private contextual attributes are decrypted using said proper first securely shared secret key (col. 23 lines 51-59, and col. 22 lines 63-68).

As per claim 23, Sudia discloses the system, wherein at least one predetermined parameter is contained in at least a portion of said decrypted private contextual attributes (col. 23 lines 51-59).

As per claim 24, Sudia discloses the system, wherein at least one predetermined parameter and said reference parameters are compared using said comparator algorithm to determine if said at least one predetermined parameter and said reference parameters match (col. 23 lines 51-59, and col. 22 lines 63-68).

As per claim 25, Sudia discloses the system, wherein a failure to achieve a match invalidates said key protection certificate (col. 10 lines 13-17).

As per claim 28, Sudia discloses the system, wherein said receiving party possesses said proper securely shared secret keys and said proper public key (col. 12 lines 13-col. 13 lines 50).

As per claim 29, Sudia discloses the system, wherein said receiving party is a trusted third party certificate authority (col. 7 lines 1-3).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia et al. (Sudia, Patent No.: US 6,209,091 B1) in view of Schell et al. (Schell Patent No.: US 6,751,735 B1).

As per claim 1, Sudia teaches a data processing system for generating a key protection certificate comprising:

a PSD (Fig. 3 No. 55) further comprising a unique device name (col. 6 lines 28-30, 45-47, 57-61, col. 9 lines 17-21), cryptography means (fig. 3 No. 46), data processing means (fig. 3 No. 44), data storage means (fig. 3 No. 52) and communications means (fig. 3 No. 42);

wherein said cryptography means includes an asymmetric cryptographic key pair generating algorithm (col. 6 lines 57-65), a first securely shared secret key, a second securely shared secret key (col. 12 lines 18-col. 13 lines 50), a concatenation algorithm (col. 17 lines 32-33), a message authentication code algorithm (col. 2 lines 16-44, col. 2 lines 52-67, col. 17 lines 39-42, and col. 18 lines 65-67), cryptographic seed information (col. 12 lines 47-49), a key protection certificate generating algorithm (col. 9 lines 37-57and col. 12 lines 47-49) a signing algorithm (fig. 2 NO. 39), and

wherein said key protection certificate generating algorithm comprises means for producing sequentially with said cryptographic key generating algorithm (col. 2 lines 49-67, and fig. 24), upon completion of cryptographic key generation and in dependence on said generated cryptographic key, a unique digital certificate that comprises said unique device name (col. 8 lines 36-58, and col. 14 lines 1-4).

Sudia fail to explicitly teach symmetric cryptography means,

However Schell discloses symmetric cryptography means (Schell col. 13 lines 22-27),

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Schell within the system of Sudia because

they are analogous in sequentially generating a digital certificate and authentication (Schell fig. 5). One in the art would have been motivated to incorporate the teaching of Schell into Sudia because it would reduce the risk of theft of signing devices and forging a signature by multi-step signing process (Schell col. 21 lines 46-50).

As per claim 2, Sudia and Schell teach all the subject matter. In addition Sudia discloses the system, wherein at least a portion of said cryptographic seed information is used by said asymmetric key pair-generating algorithm to generate at least one asymmetric private key and one asymmetric public key upon receipt of at least one key generation command, said keys being stored in a secure domain of said PSD (col. 6 lines 54-67, col. 6 lines 45-65, col. 29 lines 24-37).

As per claim 3, Sudia and Schell teach all the subject matter. In addition Sudia discloses the system, wherein said key protection certificate generating algorithm, upon receipt of said key generation command, generates a plurality of contextual attributes (col. 23 lines 46-59).

As per claim 4, Sudia and Schell teach all the subject matter. In addition Sudia discloses the system, wherein at least a portion of said contextual attributes are encrypted using said first shared secret key and said symmetric cryptography means to generate private contextual attributes (col. 23 lines 28-51).

As per claim 5, Sudia and Schell teach all the subject matter. In addition Sudia discloses the system, wherein the remaining unencrypted of said plurality of said contextual attributes forms public contextual attributes (col. 6 lines 53-65).

As per claim 6, Sudia and Schell teach all the subject matter. In addition Sudia discloses the system, wherein a signed device name is generated using said unique device name and said asymmetric private key as inputs into said signing algorithm (col. 14 lines 1-4).

As per claim 7, Sudia and Schell teach all the subject matter. In addition Sudia discloses the system, wherein said private contextual attributes, public contextual attributes, signed device name and unique device name are concatenated by said concatenation algorithm, generating a first intermediate result (fig. 6 No. 107, col. 26 lines 12-13; Header including a clear unique device name is combined with private and public contextual attributes, and digital signature to form a first intermediate result).

As per claim 8, Sudia and Schell teach all the subject matter. In addition Sudia discloses the system, wherein a message authentication code is generated using said second shared secret key and said first intermediate result as inputs into said message authentication code algorithm, forming a second intermediate result (col. 14 lines 16-44; hash is generated to form a second intermediate result).

As per claim 9, Sudia and Schell teach all the subject matter. In addition Sudia discloses the system, wherein said first intermediate result and said second intermediate result are concatenated by said concatenation algorithm forming said key protection certificate then stored in said secure domain of said PSD (col. 14 lines 16-57, col. 15 lines 59-64; hash is combined with the header including a clear unique device name, private and public contextual attributes, digital signature to form a first intermediate result and stored).

As per claim 10, Sudia and Schell teach all the subject matter. In addition Sudia discloses the system, wherein said unique device name is an embedded serial number (col. 14 lines 1-4).

As per claim 11, Sudia and Schell teach all the subject matter. In addition Sudia discloses the system, wherein said unique device name is the result of a cryptographic process using said embedded serial number as a cryptographic seed (col. 26 lines 1-13).

As per claim 12, Sudia and Schell teach all the subject matter. In addition both discloses the system, wherein said communications means includes means for receiving commands to generate asymmetric (Sudia, col. 12 lines 18-col. 13 lines 50) and symmetric keys and means (Schell col. 13 lines 22-27) for sending said public key and said key protection certificate (col. 14 lines 41-45).

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
May 18, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100